REMARKS

Reconsideration and further examination of the present application is respectfully requested. At the time the Office Action was mailed claims 1-9, 12, 14, 16-17, 20, 22-32, and 34-66 were pending. By way of the present response the Applicant has: 1) amended claims 1, 23, 50, 57, and 62; 2) added no new claims; and 3) canceled claims 32, 34, and 37-43. As such, Claims 1-9, 12, 14, 16-17, 20, 22-32, 35-36, 44-66 are now pending. Applicant respectfully requests reconsideration of the present application and the allowance of all claims.

35 USC 103(a)

Claims 1-9, 12, 14, 16-17, 20, 22-32, and 34-66 were rejected as being unpatentable over Glover, US Pat. No. 6,763,466 (hereinafter "Glover") in view of Freund, US Pat. No. 5,987,611 (hereinafter "Freund").

Glover describes that "anti-virus state information is stored within an associated data structure that is created and/or maintained by the file system of [a] computer." (Glover, Abstract.) "When the file 307 is created by the file system, the anti-virus program 305 scans 1 the file for known viruses. The anti-virus program 305 stores 2 AV state information 315 in the reserved fields 313 in the entry data structure 309 for the file 307." (Glover, Col. 6, lines 17-22.) "When the file 307 is next accessed, the entry data structure 309 is automatically read into memory by the file system, if it is not already cached. The anti-virus program 305 obtains 3 the AV state information 315 from the reserved fields 313 (decrypting it, if necessary) and compares the saved AV state information with the corresponding information currently associated with the file. If the current information is different from that stored in the AV state information 315, the file 307 is re-scanned 4 and the AV state information 315 is updated 2 with the results. Furthermore, access to the file 307 may be limited or refused by the operating system if the AV state information 315 indicates the file is infected." (Glover, Col. 6, lines 41-52.) Thus, Glover is simply an anti-virus program on a single computer.

Freund describes a "system... preferably ... capable of restricting access to the Internet (or other Wide Area Network) to certain approved applications or/and application versions." (Freund, Col. 8, lines 45-47.) "The system should preferably be capable of filtering incoming data, including binary files, for detecting viruses and Trojan

Horse programs." (Freund, Col. 9, lines 14-16.) "By monitoring abilities of individual applications to access the Internet and limiting such access to approved applications only, the Internet access monitoring system of the present invention can greatly reduce or eliminate the risk of such [intentionally destructive] attacks." (Freund, Col. 11, lines 5-9.) "In accordance with the present invention, a central filter is not employed." (Freund, Col. 12, lines 48-49.)

Thus the combination of Glover and Freund would be a computer "that preferably has present" the anti-virus of Glover as well as the access control on a per application basis of Freund. However, since the anti-virus of Glover is scanning files on the machine, the access control on a per application basis of Freund would have no interaction with the anti-virus of Glover, with the exception of the Freund access control system requiring the anti-virus of Glover to be up-to-date for the anti-virus software to access the internet. Whether or not the anti-virus program of Glover is up-to-date does not influence whether or not the Freund access control system allows any other program to access the internet.

Examiner Interview

Applicant thanks the Examiner for conducting an interview with respect to this Office Action on October 24, 2005. During the interview, the claims as presented herein (those amended and unamended) were discussed, and the Examiner indicated that all of Applicant's independent claims overcome the 103 rejections of the Office Action. Applicant respectfully submits exemplary limitations of these allowable claims:

In claim 1:

> the access module coupled to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the at least one host device using the communication module of the at least one host device, and, if the status of the anti-virus protection of the at least one host device is not compliant with the policy, to deny the at least one host device access to the Internet and to bring the anti-virus protection of the at least one host device into compliance with the policy.

In claim 44:

> the access module coupled to the LAN to maintain a

policy regarding anti-virus protection for the LAN and
manage anti-virus protection scanning performed by the at
least one host device, the access module to exchange anti-
virus protection information with the at least one host
device using the communication module of the at least host
device and to deny the at least one host device access to the
Internet if the at least one host device does not have anti-
virus protection compliant with the policy, wherein
compliance with the policy is either a range of compliance
or the most up to date anti-virus protection depending on
whether there is currently a virus alert.

The remaining dependent claims are allowable for at least the same rationale.

Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance.

Invitation for a telephone interview

The Examiner is invited to call the undersigned at 408-720-8300 if there remains any issue with allowance of this case.
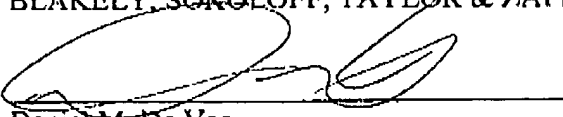
Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: _____10/26_____, 2005

Daniel M. De Vos
Reg. No. 37,813

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025-1026
(408) 720-8300

Attorney's Docket Number: 4619.P001   17   Appl. Ser. No. 09/835,054

PAGE 21/21 * RCVD AT 10/26/2005 6:02:11 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID:408 720 9397 * DURATION (mm-ss):04-30